Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性(CVE-2019-1735)

Medium

アドバイザリーID : cisco-sa-20190515-nxos-cmdinj-1735　CVE-2019-1735
初公開日 : 2019-05-15 16:00
最終更新日 : 2021-07-12 14:24
バージョン 1.1 : Final
CVSSスコア : 4.4
回避策 : No workarounds available
Cisco バグ ID : CSCvj63728 CSCvk52972 CSCvk52971 CSCvk52969 CSCvk52988 CSCvj63877 CSCvk52975 CSCvk52985

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco NX-OSソフトウェアのCLIにおける脆弱性により、認証されたローカルの攻撃者が、該当デバイスの基盤となるオペレーティングシステム上で、権限を昇格させた上で任意のコマンドを実行する可能性があります。

この脆弱性は、特定の CLI コマンドに渡される引数が十分に検証されないことに起因しています。攻撃者が、該当コマンドの引数として悪意のある入力を含めることにより、この脆弱性を工クスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者は昇格された特権を使用して基盤となるオペレーティング システムで任意のコマンドを実行できるようになります。攻撃者がこの脆弱性をエクスプロイトするには、有効なユーザ クレデンシャルが必要です。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cmdinj-1735

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 1000仮想エッジ
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Nexus 9500 R シリーズ スイッチング プラットフォーム
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6400 シリーズ ファブリック インターコネクト

脆弱性が存在する Cisco NX-OS ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- Nexus 9000 シリーズ ファブリック スイッチ（アプリケーション セントリック インフラストラクチャ（ACI）モード）

詳細

シスコは、同様のCLIコマンドインジェクションの脆弱性をいくつか公開しています。主に影響を受ける製品とソフトウェアバージョンが異なります。次の表に、Cisco Bug IDおよびCVE IDによる各脆弱性の該当製品を示します。

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
Cisco NX-OSソフトウェアラインカードのコマンドインジェクションの脆弱性 (CVE-2019-1769)	N/A	N/A	N/A	0.CSCvh20032	0.CSCvj00299	N/A	N/A
Cisco NX-OSソフトウェアのコマンドインジ	N/A	CSCvh75867[1]	0.CSCvi92240 0.CSCvk36294	0.CSCvh75958 0.CSCvi92242	0.CSCvi92239	0.CSCvi92243	N/A

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
ェクションの脆弱性 (CVE-2019-1770)							
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1774、CVE-2019-1775)	N/A	0.CSCvh75895 0.CSCvh75909	N/A	0.CSCvh75968 0.CSCvh75976 0.CSCvi99197 0.CSCvi92258	0.CSCvi99195 0.CSCvi92256	0.CSCvi99198 0.CSCvi92260	N/A

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1776)	N/A	0.CSCvh20081	N/A	0.CSCvh20076 0.CSCvi96431	0.CSCvi96429	0.CSCvi96432	CSCvi96433[2]
Cisco NX-OSソフトウェアのコマンドインジェクションの	N/A	N/A	N/A	0.CSCvh75996	0.CSCvj03877	N/A	N/A

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
脆弱性 (CVE-2019-1778)							
Cisco FXOSおよびNX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1779)	0.CSCvj00418	0.CSCve51688	N/A	0.CSCvh76126	0.CSCvj00412	0.CSCvj00416	N/A
Cisco FXOSおよび	0.CSCvi92332	0.CSCvi01440	N/A	0.CSCvi01431 0.CSCvi92328	0.CSCvi92326	0.CSCvi92329	N/A

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1780)							
Cisco FXOSおよびNX-OSソフトウェアのコマンドインジェクシ	0.CSCvi96527 0.CSCvi92130	0.CSCvi01448 0.CSCvh20389	N/A	0.CSCvi01445 0.CSCvh20027 0.CSCvi96524 0.CSCvi92126	0.CSCvi96522 0.CSCvi91985	0.CSCvi96525 0.CSCvi92128	CSCvi96526[2] CSCvi92129[2]

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性(CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
ョンの脆弱性(CVE-2019-1781、CVE-2019-1782)							
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性(CVE-2019-1783)	N/A	CSCvi42281[1]	N/A	N/A	N/A	0.CSCvj03966	N/A
Cisco	N/A	CSCvi42292[1]	N/A	N/A	N/A	0.CSCvj12273	CSCvj12274[2]

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1784)							
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性	N/A	0.CSCvh20112	N/A	0.CSCvh20096	0.CSCvi96504	0.CSCvi96509	CSCvi96510[2]

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
(CVE-2019-1790)							
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性 (CVE-2019-1791)	N/A	0.CSCvj63667	N/A	0.CSCvj63270 0.CSCvk50873	0.CSCvk50889	0.CSCvk50876	N/A
Cisco FXOSおよびNX-OSソフトウェ	0.CSCvh66259	0.CSCvh20359	0.CSCvh66257 0.CSCvk30761	0.CSCvh20029 0.CSCvh66219	0.CSCvh66202	0.CSCvh66214	CSCvh66243[2]

セキュリティアドバイザリ	FP 4100/ 9300	MDS 9000/ N7K/ 7700ナイラ[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	3600ナイラ/ N9500R	55億ナイラ/ 5600ナイラ/ N6K	UCS 6200/ UCS 6300 UCS 64002
Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性(CVE-2019-1735)	N/A	0.CSCvj63728	0.CSCvk52969 0.CSCvk52985	0.CSCvj63877 0.CSCvk52971	0.CSCvk52988	0.CSCvk52972	0.CSCvk52975
アのコマンドインジェクションの脆弱性(CVE-2019-1795)							

1. CSCvh75867、CSCvi42281、およびCSCvi42292は、Nexus 7000シリーズおよびNexus 7700シリーズスイッチにのみ適用されます。MDS 9000シリーズマルチレイヤスイッチは、これらの脆弱性の影響を受けません。
2. CSCvk52975は、UCS 6200、6300、および6400に適用されます。他のすべてのUCS不具合では、UCS 6200と6300のみが該当します（UCS 6400は該当しません）。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスを

ご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は https://www.cisco.com/c/en/us/products/end-user-license-agreement.html に記載のシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

2019年3月のCisco FXOSおよびNX-OSソフトウェアバンドルに対応する推奨リリースをすでに適用しているお客様は、アップグレード操作を行う必要はありません。バンドルされているアドバイザリのリストについては、『Cisco Event Response: 2019年3月Cisco FXOSおよびNX-OSソフトウェアのセキュリティアドバイザリバンドル公開』を参照してください。

2019年3月のバンドルに対応する推奨リリースを適用していないお客様は、このセクションの該当する表に示されているように、適切なリリースにアップグレードすることをお勧めします。次の表では、左の列にCisco NX-OSソフトウェアリリースを示します。右の列は、この脆弱性が修正済みの最初の推奨リリースです。

MDS 9000シリーズマルチレイヤスイッチ：CSCvj63728

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
5.2	6.2(29)
6.2	6.2(29)
8.1	8.3(1)
8.2	8.3(1)
8.3	8.3(1)

Nexus 1000仮想エッジ：CSCvk52969

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
5.2	5.2(1)SV5(1.1)

Microsoft Hyper-V向けNexus 1000Vスイッチ：CSCvk52985

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
5.2 より前	公開済みの修正プログラムはありません
5.2	公開済みの修正プログラムはありません

VMware vSphere用Nexus 1000Vスイッチ：CSCvk52969

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
5.2 より前	5.2(1)SV3(4.1a)
5.2	5.2(1)SV3(4.1a)

スタンドアロンNX-OSモードのNexus 3000シリーズスイッチおよびNexus 9000シリーズスイッチ：CSCvj63877

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
7.0(3)I4 よりも前	7.0(3)I4(9)
7.0(3)I4	7.0(3)I4(9)
7.0(3)I7	7.0(3)I7(6)
9.2(1)	脆弱性なし

Nexus 3500プラットフォームスイッチ：CSCvk52971

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
6.0(2)A8 より前	6.0(2)A8(11)

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
6.0(2)A8	6.0(2)A8(11)
7.0(3)I4	7.0(3)I4(9)
7.0(3)I7	7.0(3)I7(6)
9.2	脆弱性なし

Nexus 3600プラットフォームスイッチおよびNexus 9500 Rシリーズスイッチングプラットフォーム：CSCvk52988

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
7.0(3)	7.0(3)F3(5)
9.2	脆弱性なし

Nexus 5500および5600プラットフォームスイッチと6000シリーズスイッチ：CSCvk52972

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
7.3	7.3(4)N1(1)
7.3	7.3(4)N1(1)

Nexus 7000および7700シリーズスイッチ：CSCvj63728

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
6.2 より前	6.2(22)
6.2	6.2(22)
7.2	7.3(3)D1(1)
7.3	7.3(3)D1(1)
8.0	8.3(1)
8.1	8.3(1)
8.2	8.3(1)
8.3	8.3(1)

UCS 6200、6300、および6400シリーズファブリックインターコネクト：CSCvk52975

Cisco NX-OS ソフトウェアリリース	この脆弱性に対する最初の修正リリース
4.0	4.0(2a)
4.0	4.0(2a)

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの決定に関してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。 セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
VMware 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 シリーズおよび 3500 シリーズ スイッチ
Cisco Nexus 5000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に最適な Cisco NX-OS ソフトウェア リリースの確認に関してサポートが必要な場合は、デバイスのリリース ノートに記載されている推奨リリースに関するドキュメントを参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cmdinj-1735

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	MDS 9000シリーズマルチレイヤスイッチの修正済みリリース情報を更新。	修正済みソフトウェア	Final	2021年7月12日
1.0	初回公開リリース	—	Final	2019年5月15日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。